IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

SYCURIO LIMITED and SYCURIO INC. Plaintiffs, v. PCI PAL (U.S.) INC., Defendant.	DOCKET NO. 3:21-cv-00486-MOC-DSC **STIPULATION AND AGREED ORDER REGARDING DISCOVERY AND USE OF ELECTRONICALLY STORED INFORMATION**

This Protocol Regarding Disclosure of Electronically Stored Information ("Protocol") governs the disclosure of ESI in this Litigation.

1.   This Protocol is meant to streamline Electronically Stored Information ("ESI") production to promote an efficient, less burdensome process and in accordance with the standard set forth in Federal Rule of Civil Procedure 26. Except as expressly stated, nothing in this Protocol affects the parties' discovery obligations in this proceeding.

I.   GENERAL PROVISIONS

2.   Any documents collected from hard copies shall be produced as they are maintained in the ordinary course of business along with a scanned image of their original folders, binders, covers or containers thereof, i.e., documents shall be produced electronically in the manner in which such documents were stored and retrieved in hard copy form. The responding party is not required to append a copy of each image of the folders, binders, covers, or containers to each document taken from the same file, though, upon request, the parties will identify by bates number documents that were contained within a specific folder or binder from which hard copies were collected.

1

4874-0987-8334.9

3.   Modification. This Protocol may be modified by agreement of the parties. If the parties cannot agree regarding any such modifications, the parties shall submit their competing proposals and a summary of their dispute to the Court.

4.   Cost-Shifting. The parties agree to bear their own ESI-related discovery costs for any list of custodians and search parameters upon which the parties initially agree. After the initial extraction of materials is complete, parties may request that additional custodians or terms be searched and the parties will confer as to who bears the costs for any additional searches. If the parties cannot agree, either party may request that the Court determine that cost-shifting is warranted due to a party's unwarranted ESI production requests or other failure to comply with the letter and spirit of this Protocol. A party's meaningful compliance with this Protocol and efforts to promote efficiency and reduce costs will be considered in any cost-shifting determination.

5.   Reasonable Efforts. The parties will make reasonable efforts to prepare responsive and non-privileged data for production in accordance with the agreed-upon specifications set forth below. These specifications apply to scanned, hard copy documents and/or ESI that are to be produced in this litigation.

6.   Data Not Reasonably Accessible. Absent a showing of good cause, no party need restore any form of media upon which backup data is maintained in a party's normal or allowed processes, including but not limited to back up tapes, disks, SAN, and other forms of media, to comply with its discovery obligations in the present case.

7.   Other Excluded ESI. Absent a showing of good cause by the requesting party, the categories of ESI identified in Schedule A attached hereto need not be preserved.

8.   Information Subject to a Claim of Privilege. Subject to Paragraph 9, any document/ESI falling within the scope of any request for production or subpoena that is withheld

on the basis of a claim of attorney-client privilege, work-product or any other claim of privilege or immunity from discovery shall be identified by the producing party in a privilege log, which the producing party shall produce in an electronic format that allows text searching and organization of data. An email thread contained within a single document need only be recorded once on the producing party's privilege log, even if a privilege is asserted over multiple portions of the thread.

9. No privilege log identification is required for the following categories of communications exchanged on or after the date of filing of Claim No. HP-2021-000030 pending before the High Court of Justice in the United Kingdom:

      a. Communications between the producing party's outside or in-house counsel and employees of the producing party;

      b. Communications between the producing party's outside or in-house counsel and former employees of the producing party concerning matters that were within the scope of the former employees' corporate duties; and

      c. Communications between outside counsel for the producing party.

For the avoidance of doubt, any communications involving individuals who are not employees of the producing party or former employees under sub-paragraph (b) must be logged. Members of a producing party's board of directors shall be considered employees for purposes of this paragraph. The contents of the privilege log shall include the information required by Federal Rule of Civil Procedure 26(b)(5).

10. Pursuant to Rule 502(d) of the Federal Rules of Evidence, production of privileged or work-product-protected documents or ESI does not constitute a waiver in the pending case or in any other federal or state proceeding.

3

11.   The mere production of documents or ESI in a litigation as part of a mass production shall not itself constitute a waiver for any purpose.

12.   Redactions. Documents that contain both privileged and non-privileged information will be produced with the privileged information redacted in such a way as to show the location of the redaction within the document and the reason therefore (*e.g.*, *"Redacted – Privileged" or equivalent*). Subject to Paragraph 9, documents or portions thereof withheld on privilege grounds will be identified in a privilege log in accordance with Federal Rule of Civil Procedure 26(b)(5). Additionally, portions of documents withheld on privilege grounds need not be identified in a privilege log as long as sufficient information remains on the face of the document to provide the opposing party with the type of information that would otherwise be included on a privilege log entry.

13.   English Language. To the extent any data exists in more than one language, the data shall be produced in English, if available. If no English version of a document is available, the producing party does not have an obligation to produce an English translation of a document.

14.   Format of Production. Hard copy documents will be produced under the specifications outlined in Section III. Standard electronic files such as email, documents, spreadsheets, presentations, web pages, and PDFs will be produced under the specifications outlined in Section IV. The format of production of any large oversized hard copy documents and non-standard electronic files will be discussed before production to determine acceptable production format.

II.   DATA PROCESSING

15.   Culling and Filtering. Each party will use reasonable efforts to filter out common system files and application executable files by using a commercially reasonable hash

identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list. Additional culling of system file types based on file extension may include, but are not limited to: WINNT, DRVS, MP3, MP4, WAV, C++ Program File (c), C++ Builder 6 (cpp), Channel Definition Format (cdf), Creatures Object Sources (cos), Dictionary file (dic), Executable (exe), Hypertext Cascading Style Sheet (css), JavaScript Source Code (js), Label Pro Data File (IPD), Office Data File (NICK), Office Profile Settings (ops), Outlook Rules Wizard File (rwz), Scrap Object (SCRP), System File (dll), Temporary File (tmp), Windows Error Dump (dmp), Windows Media Player Skin Package (wmz), Windows NT/2000 Event View Log file (evt), Python Script files (.py, .pyc, .pud, .pyw), Program Installers. None of these culling/filtering options shall relieve a party of its duty to produce source code or other files sufficient to show the operation of any aspects or elements of any relevant software, product, device, process, method, act, or other instrumentality.

16.   De-Duplication. The producing party shall de-duplicate across the population of records (i.e., global de-duplication). Duplicates for non-email data sources shall be identified by industry standard MD5 or SHA-1 hash value only. For email files, duplicate email files shall be identified based upon a commercially accepted method for the email family, which includes the parent email and attachments. Duplicate messaging materials will be identified at a family level, including message and attachment(s). Any other methodology for identification of duplicates must be discussed with the receiving party and approved in writing before implementation. However, duplicates (or equivalent identifying information) must be produced where necessary to preserve parent/child relationships. A party producing a document in electronic form need not produce the same document in hard copy or paper format.

17.   Parent-Child Relationships. Parent-child relationships (the association between an attachment and its parent document) that have been maintained in the ordinary course of business must be preserved. For example, if a party is producing an email that has attachments, the attachments shall be processed in order behind the email. Parent/child relationships will be maintained using the BEGATTACH and ENDATTACH metadata fields.

III.   PRODUCTION OF HARD COPY DOCUMENTS

18.   Unless requests call for the production of hard copy documents that are difficult to convert or for legibility or clarity purposes are better rendered in hard copy format, subject to the parties' duty to meet and confer about any disputes, the parties shall convert hard copy documents to an electronic format for production.

19.   TIFFs. Documents that exist only in hard copy format shall be scanned and produced as single page TIFFs at a resolution of at least 300 dots per inch (dpi). Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed upon confidentiality designation. TIFFs shall show all text and images that would be visible to a user of the hard copy documents. The parties will accommodate reasonable requests for production of specific images in color or higher resolution. Nothing in this Protocol shall preclude a producing party from objecting to such requests as unreasonable in number, timing or scope, provided that a producing party shall not object if the document as originally produced is unreadable. If a document is originally produced in an unreadable form, the producing party shall have the option of responding by producing a native-file version of the document or producing a replacement image of legible quality. If a dispute arises with regard to requests for higher resolution or color images, the parties will meet and confer in good faith to try and resolve it.

6

20. Unitizing of Documents. In scanning hard copy documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., hard copy documents should be logically unitized). The parties will use reasonable efforts to unitize documents correctly.

21. OCR Text Files. A commercially acceptable technology for optical character recognition "OCR" shall be used for all scanned, hard copy documents (other than redacted documents). OCR text shall be provided as a document level text file for each document, and the filename should match its respective TIFF filename. The text files will not contain the redacted portions of the documents.

22. Metadata Fields. The following information shall be produced in the delimited data file accompanying hard copy documents: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH, (e) CONFIDENTIALITY, and (f) CUSTODIAN.

23. Database Load Files/Cross-Reference Files. Productions shall include, in addition to single page TIFFs and Text Files, (a) an ASCII delimited data file (.txt, .dat, or .csv), and (b) an image load file (.opt or .lfp) that can be loaded into commercially acceptable production software (e.g., Concordance, Relativity). Each TIFF in a production must be referenced in the corresponding image load file. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s) in the production.

24. Bates Numbering. All documents produced either in hard copy or TIFF images must be assigned a unique Bates number that is sequential within a given document and across the production sets.

IV.   PRODUCTION OF ELECTRONICALLY STORED INFORMATION

25.   <u>Metadata Fields and Processing</u>. The parties agree that load files should include, where applicable, the information listed in the table of metadata fields, set forth in Schedule B below. However, the parties are not obligated to include metadata for any document that does not contain such metadata in the original. The parties reserve their rights to object to any request for the creation of metadata for documents that do not contain metadata in the original.

26.   <u>TIFFs</u>. Except as otherwise provided for in this Protocol, all documents existing in electronic format shall be produced in either native form or as single-page TIFF format at a resolution of at least 300 dots per inch (dpi). TIFF files shall be produced along with Concordance/Opticon image load files that indicate the beginning and ending of each document. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed upon confidentiality designation (if applicable). Reasonable efforts shall be made to preserve original document orientation (i.e., portrait to portrait and landscape to landscape) and all text and images that would be visible in the original electronic format including redlines and speaker notes, but reasonable effort shall not include or require any individual hand-processing of files.

27.   <u>Text Files</u>. A single multi-page text file shall be provided for each document, and the filename should match its respective TIFF filename. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents, and OCR text files will be substituted instead of extracted text files for redacted documents.

28.   <u>Database Load Files/Cross-Reference Files</u>. Productions shall include, in addition to single page TIFFs and Text Files, (a) an ASCII delimited data file (.txt, .dat, or .csv), and (b) an

8

image load file that can be loaded into commercially acceptable production software (e.g., Concordance, Relativity). Each TIFF in a production must be referenced in the corresponding image load file (.opt or .lfp). The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s) in the production. Load file information may be provided in a supplemental overlay file as designated on Schedule B, Column "Supplemental Overlay (Y/N)."

29.   Proprietary Files. To the extent a response to discovery requires production of ESI accessible only through proprietary or licensed software, including but not limited to accounting records, testing or development records, or a quotation database, the parties shall confer and agree on a report containing information or the retrieval of relevant specific documents relevant to the request. The parties should continue to preserve the information associated with such databases unless the failure to preserve has been disclosed and agreed upon between the parties. Similarly, to the extent that decryption or access passwords are necessary to unlock any data in its native format, including but not limited to e-mail passwords and file decryption passwords, the parties shall meet and confer to develop appropriate steps to allow access to the data without compromising confidentiality, security, or proprietary interests. The parties shall meet and confer to finalize the appropriate production format for proprietary files.

30.   Request(s) for Additional Native Files. The parties agree to respond to reasonable and specific requests for the production of certain files in native format. If a dispute arises with regard to requests for the production of files in native format, the parties will meet and confer in good faith to try and resolve it. If the parties are unable to reach agreement with regard to requests for additional documents in native-file format, the parties reserve the right to seek relief from the

Court. Excel files, Powerpoint files, and files failing to generate TIFF images (executables, multi-media, etc.) shall be produced in native file format. Any native files that are produced shall be produced with a link in the Native Link field, along with extracted text and applicable metadata fields set forth in Schedule B. A TIFF placeholder indicating that the document was provided in native format should accompany the database record. The TIFF placeholder should also indicate the Bates number and confidentiality designation (if applicable) assigned to the native document. If a file has been redacted, TIFF images and OCR text of the redacted document will suffice in lieu of a native file and extracted text.

31. <u>Redaction of Information</u>. If documents are produced containing redacted information, an electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration or addition the content of such data including any metadata therein.

V. PROCESSING OF THIRD-PARTY DOCUMENTS

32. Subpoena. A party that issues a non-party subpoena ("Issuing Party") shall include a copy of this Protocol and the Agreed Confidentiality Order with the subpoena and state that the parties to the litigation urge that third parties produce documents in accordance with the specifications set forth herein. However, nothing in this Protocol is intended to or should be interpreted as narrowing, expanding, or otherwise affecting the rights of the parties or third parties to object to a subpoena. If the subpoenaed party produces documents only to the Issuing Party or produces in a format not in accordance with the specifications of this Protocol, the Issuing Party must provide exact copies to the other parties in a format from which they can reasonably access the documents within five business days of receipt.

33.   Production Not Bates-Stamped. If the non-party production is not Bates-stamped, the Issuing Party will endorse the non-party production with unique prefixes and Bates numbers and provide them to the opposing party within ten business days of receipt.

VI.   REQUIRED SEARCHES

34.   General ESI production requests under Federal Rules of Civil Procedure 34 and 45 shall not include email or other forms of electronic correspondence (collectively "email"). To obtain email, parties must propound specific email production requests. Each party must identify and produce non-email ESI that is responsive to any discovery requests under Federal Rules of Civil Procedure 34 and 45 notwithstanding the email search provisions set forth in this section.

35.   The parties will cooperate to identify a date for the mutual exchange of email production requests.

36.   Email production requests shall only be propounded for specific issues, rather than general discovery of a product or business.

37.   Each email production request shall identify the specific issue and relevant time frame if known.

38.   Upon receipt of the email production requests, the parties shall negotiate in good faith to identify and agree on appropriate custodians, search terms and timeframe(s) likely to yield a reasonable number of relevant, responsive, non-privileged communications proportional to the needs of the case. During such negotiations, the parties shall exchange hit counts for proposed search terms and using this information, work to promote efficiency and avoid undue burden.

39.   The parties shall confer on a process to test the efficacy of the search terms and mutually agree on an appropriate number of search terms applying to each side. The search terms shall be narrowly tailored to particular issues. Indiscriminate terms, such as the producing

11

company's name or its product name, are inappropriate unless combined with narrowing search criteria that sufficiently reduce the risk of overproduction. A conjunctive combination of multiple words or phrases (e.g., "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (e.g., "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term unless they are variants of the same word. Use of narrowing search criteria (e.g., "and," "but not," "w/x") is encouraged to limit the production and shall be considered when determining whether to shift costs for disproportionate discovery.

40.   However, the parties recognize that, despite their best efforts to agree on narrowly tailored search terms, it may be difficult to determine in advance how many documents will be "hit" by a particular set of search terms until after the email searches are performed. In the event that the producing party discovers that a search term or terms would result in a number of documents for review that would present an excessive or undue burden, the parties are to meet and confer in good faith to determine whether additional modifications to those search terms (e.g., the addition of narrowing search criteria such as "and" and "but not") can be made. For the avoidance of doubt, where the narrowing criteria include disjunctive combinations, such disjunctive terms shall not constitute separate search terms.

41.   Nothing in this Order prevents the parties from agreeing to use technology assisted review and other techniques insofar as their use improves the efficacy of discovery.
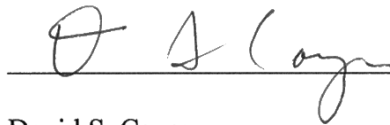
VII.   EMAIL THREADING

42.   Email threads are email communications that contain prior or lesser-included email communications that also may exist separately in the Party's electronic document collection. A most-inclusive email is one that contains unique content and all of the lesser-included emails,

12

including attachments, for that branch of the email thread. The Parties agree that removal of lesser-included versions from potential production will reduce all Parties' costs of document review, production, and litigation-support hosting. Accordingly, each Party may produce only inclusive email threads from each and every email branch.

SO ORDERED.

Signed: December 21,

David S. Cayer
United States Magistrate Judge

SCHEDULE A

1.   Deleted, slack, fragmented, or other data only accessible by forensics.

2.   Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

3.   On-line access data such as temporary internet files, history, cache, cookies, and the like.

4.   Data in metadata fields that are frequently updated automatically, such as last-opened dates.

5.   Back-up data that are substantially duplicative of data that are more accessible elsewhere.

6.   Voice messages to the extent saved only on a mobile device or voice messaging server.

7.   Instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging.

8.   Pin-to-pin messages, iMessages, or other text messages sent to or from mobile devices or through apps installed on mobile devices (e.g., WhatsApp, Google Hangouts).

9.   Other electronic data stored on a mobile device, such as calendar or contact data or notes, provided that a copy of such information is routinely saved elsewhere.

10.   Logs of calls made from mobile devices.

11.   Server, system or network logs.

12.   Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report.

13.   Data remaining from systems no longer in use that is unintelligible on the systems in use.

14

SCHEDULE B: METADATA FIELDS

Load file names, field names, folder names may be different than what has been specified below so long as substantially the same information is provided, and a cross reference sheet of the names are provided on request. Supplemental overlay files will not be provided without prior agreement as to which party will bear any cost for creating/extracting the specified metadata. To the extent a party seeks to impose the costs of supplemental overlay metadata fields on the non-producing party, the producing party shall provide an estimate from an e-discovery vendor of the costs of providing each additional metadata field reasonably in advance of the document production.

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
CUSTODIAN/SOURCE	Includes the Individual (Custodian) or Non-Custodial Source from whom/which the documents originated
ALL CUSTODIAN (or GLOBALSOURCE)	A semi-colon delimited list of all Custodians and Non-Custodial Sources in possession of a document (i.e., all Individual(s)/sources from whom/which documents were de-duplicated out (De-Duped Custodian)
SUBJECT	Subject from properties of document
TITLE	Title from properties of document
DATESENT	Date email was sent (format: MM/DD/YYYY)
TIMESENT	Time email was sent (in EST; format: HH:MM:SS)
TO	All recipients that were included on the "To" line of the email
FROM	The name and email address of the sender of the email
CC	All recipients that were included on the "CC" line of the email
BCC	All recipients that were included on the "BCC" line of the email
EMAIL SUBJECT	From email subject line

AUTHOR	Any value populated in the Author field of the document properties
FILENAME	Filename of an electronic document (Edoc or attachment)
MD5HASH	MD5 hash value of the file
FILEPATH	Original file path showing where the document was stored. For email this should be the email folder path (e.g., johndoe.pst\Inbox\). For lose files, this should be the path to the file (e.g., Johndoe\Desktop\My Documents\)
ALLFILEPATH	Path to duplicate maintained by other Custodians/Sources
DATEMOD	Date an electronic document was last modified (format: MM/DD/YYYY) (Edoc or attachment)
TIMEMOD	Time an electronic document was last modified (in EST; format: HH:MM:SS) (Edoc or attachment)
DATECREATED	Date an electronic document was created (format: MM/DD/YYYY) (Edoc or attachment)
TIMECREATED	Time an electronic document was created (in EST; format: HH:MM:SS) (Edoc or attachment)
FILETYPE	The document file type (e.g., MS Word, Excel)
DOCTEXT	File extension for email or Edoc (e.g., .doc)
TEXTLINK	Searchable Text File Link
NATIVELINK	Native File Link (Native Files only)
CONFIDENTIALITY DESIGNATION	The confidentiality designation (if any) pursuant to the Protective Order
REDACTED	For documents containing redactions (format: Y/N)